Configure a Content Security Policy (CSP)

Content updated: 09/03/2026

This article is designated for administrators.

About

A **Content Security Policy (CSP)** is a browser security feature that helps protect a website against cross-site scripting (XSS) and other code-injection attacks. It uses an HTTP header to tell browsers which sources the site can load resources from, including scripts, styles, images, fonts, media, and embedded content.

You can configure a CSP header for your Content Hubs or legacy Video Portal site in the **Security module**.

The **Generate CSP** button provides a suggested starting value based on your site's configuration and enabled modules. Because CSP requirements also depend on your organization's integrations and customizations, review and test the generated value before enforcing it.

If `cspHeader` is empty, a security alert displays once per login session in the Configuration Management console. Administrators can dismiss it for the current session, but it displays again during subsequent sessions until `cspHeader` is populated. The alert is a recommendation to configure a CSP; it does not indicate that a security breach has occurred.

Who can use this

Administrators with access to the Configuration Management console can configure the policy.

Before you start

- Identify the resources that browsers load when users access your site. These may include scripts, styles, images, fonts, media, frames, analytics services, identity providers, integrations, and custom modules.
- Include API endpoints only when the browser connects to them directly. Server-side API calls do not need to be included in the CSP.
- Consult your organization's security or web development team if you need help reviewing or adjusting the policy.

- Test the policy in report-only mode before enforcing it. The system does not validate the policy syntax or confirm that all required resources can load.

An incomplete or overly restrictive policy can prevent legitimate resources from loading and cause parts of the site to stop working.

Understand the CSP fields

The **Security module** provides separate fields for testing and enforcing policies for the site and the Configuration Management console.

Field	Purpose
`cspHeaderReportOnlyHeader`	Tests a policy on the site without blocking resources. CSP violations display in the browser console.
`adminCspHeaderReportOnlyHeader`	Tests a separate policy for the Configuration Management console without blocking resources. CSP violations display in the browser console.
`cspHeader`	Enforces the policy on the site. This policy also applies to the Configuration Management console when `adminCspHeader` is empty.
`adminCspHeader`	Enforces a policy specifically for the Configuration Management console. When populated, it overrides `cspHeader` for the console. When empty, the console uses the policy configured in `cspHeader`.

Use nonce tokens

You can use the following tokens in any of the CSP fields:

- `'nonce-{{scriptNonce}}'` generates a random nonce that is included in script tags.
- `'nonce-{{styleNonce}}'` generates a random nonce that is included in style tags.

Enter only the policy directives. Do not include either of the following header names:

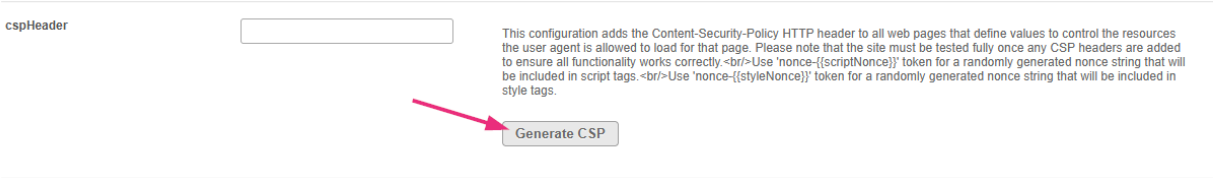
- `Content-Security-Policy:`
- `Content-Security-Policy-Report-Only:`

For descriptions of all settings, see Security module.

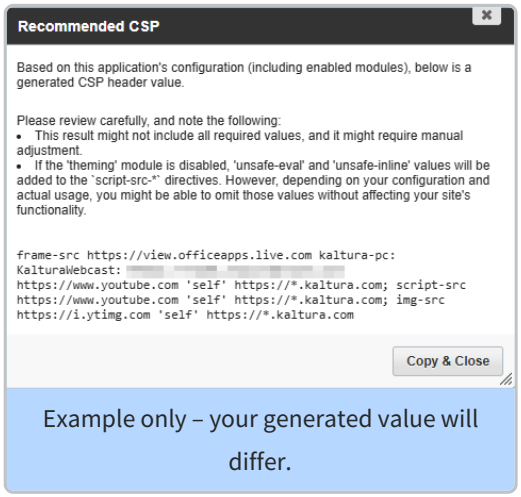
Generate a suggested CSP value

1. Log in to the **Configuration Management** console.

2. Open the **Security** module.
   The Security module settings display.
3. Click **Generate CSP** next to `cspHeader`.



   The generated CSP window displays.



Example only – your generated value will differ.

4. Review the generated value. It provides a starting policy with recommended directives, including `default-src` and `object-src 'none'`. Before applying it, check the following:

- It may not include all the sources required by your site, including sources used by custom or partner integrations.
- When the Theming module is **enabled**, the generated policy uses nonce tokens in the relevant directives instead of `'unsafe-*'` values. Keep the nonce tokens when adjusting the policy.
- When Theming is **disabled**, the generated policy includes `'unsafe-eval'` and `'unsafe-inline'` where required. Test before removing either value.

If no value is generated, do not enter or apply an empty policy. Contact Kaltura Support and include details about the site and its enabled integrations.

5. Click **Copy & Close**.

The generated value is copied, and the window closes.

Continue to the next section to test the copied value before enforcing it.

Test the policy

Use report-only mode to identify resources that the proposed policy would block without affecting site functionality.

1. Paste the copied policy directives into `cspHeaderReportOnlyHeader`.
2. If you plan to use a different policy for the Configuration Management console, enter the proposed policy in `adminCspHeaderReportOnlyHeader`.
3. Click **Save**.
   The report-only policy is applied.
4. Open your browser's developer tools, and then select the **Console** tab.
5. Test the site's main workflows, including:

- Login
- Search
- Playback
- Upload
- Embedded content
- Integrations
- Custom features

Review the CSP violation messages in the browser console. Each message identifies a resource that the policy would block and the directive responsible.

Determine whether each blocked resource is legitimate. Add trusted resources that the site requires to the appropriate directives.

- Save the updated policy and repeat the test until there are no unexpected violations.

>
> Report-only mode identifies potential problems, but it does not enforce the policy or prevent resources from loading.

Apply the policy

After you have tested and adjusted the policy:

1. In the **Security** module, copy the tested directives from

`cspHeaderReportOnlyHeader` to `cspHeader`.

2. If you tested a separate policy for the Configuration Management console, copy it from `adminCspHeaderReportOnlyHeader` to `adminCspHeader`.
3. Clear the report-only fields.
4. Click **Save**.

   The policy is enforced.

5. Test the site and Configuration Management console again to confirm that all required functionality works as expected.

After `cspHeader` contains a policy, the CSP security alert no longer displays when administrators log in to the Configuration Management console. Adding a policy only to a report-only field does not dismiss the alert.

Update or remove the policy

If the policy blocks a required resource:

1. Open the **Security** module.
2. Review the browser console to identify the blocked resource and affected directive.
3. Confirm that the resource is trusted and required.
4. Update the relevant directive, or temporarily clear the applicable enforced-policy field.
5. Click **Save**.
6. Test the affected functionality again.

If the enforced policy prevents you from accessing or using the Configuration Management console, contact Kaltura Support.